Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Informatica

LOCATOR ID SEPARATION PROTOCOL

Tesi di Laurea in Reti di Calcolatori

Relatore:
Chiar.mo Prof.
Vittorio Ghini

Presentata da:

Hassna El Filali

Sessione II
Anno Accademico 2012-2013

بسم الله الرحمن الرحيم

((وما توفيقي إلا بالله عليه توكلت و إليه أُنيب))

صدق الله العظيم

Introduzione

LISP nasce dall' esigenza di risolvere il problema della scarsa scalabilitá dei protocolli di routing e dall' inadeguatezza del sistema di indirizzamento correntemente utilizzati in Internet.

Come largamente discusso nel Routing and Addressing Workshop tenutosi ad Amsterdam in ottobre 2006, infatti, é comunemente riconosciuto che il sistema di routing e addressing della odierna Internet presenta seri problemi di scalabilitá . La sempre crescente popolazione di utenti, tanto quanto una molteplicitá di altri fattori incluso il multihoming, il traffic engeneering e le policy di routing, hanno portato ad una potenzialmente allarmante dimensione delle routing tables. La chiara ed evidente necessitá sembrerebbe quindi quella di trovare un nuovo scalabile sistema di routing e addressing che ovvi allo stesso tempo all' overloading dell' ormai sovrautilizzato singolo IP address.

Le proposte alla risoluzione dei problemi sopra enunciati si basano tutte sul concetto comune di separazione logica tra il locator e l' identifier.

LISP, difatti, propone un Protocollo di Locator/ID Separation e rappresenta quella che viene considerata una next-generation IP routing Architecture creando un nuovo paradigma nell' assegnazione e interpretazione dell' Indirizzamento IP attraverso lo splitting dell' identitá di un device, un endpoint identifier (EID) e la sua location (RLOC), in due distinti namespaces. Creando Indirizzi IP separati per EID ed RLOC, si prefigge di raggiungere determinati obiettivi, incluso quello di migliorare la scalabilitá del sistema di routing attraverso una migliore aggregazione degli RLOC e incrementare

l' efficienza del multihoming e dell' Ingress Traffic Engeneering con una gestione ottimizzata del mapping EID-to-RLOC. Tale procedura di mapping é supportata da specifici database progettati appositamente per la memorizzazione di informazioni distribuite (e.g., architetture software di tipo push, pull oppure ibride). LISP non specifica direttamente in che modo i mapping database debbano essere progettati e sviluppati in quanto essi, al fine di facilitare la sperimentazione di una grossa varietá di approcci e design differenti, costituiscono un modulo e caso di studio separato.

Il seguente elaborato é stato cosi strutturato:

• Presentazione e introduzione al Protocollo LISP con particolare riferimento alle necessitá che hanno portato alla sua formulazione e ai propositi per la relative risoluzioni: implementare il Locator/ID split (Cap. 1).

• Il Multihoming: un problema ormai alle porte. Considerazioni generali con cenni agli attuali metodi di implementazione e loro ottimizzazione in LISP (Cap. 2).

• L'infrastruttura LISP: elementi funzionali e loro descrizione operativa (Cap. 3).

• Approfondimenti sul processo di Tunneling e di trasmissione dei pacchetti con particolare riferimento agli odierni Protocolli di Trasmissione IPv4 e IPv6 (Cap. 4).

• Descrizione delle funzionalitá del Protocollo : processi di Data Plane e Control Plane. Il LISP-ALT : un particolare Lisp Control Plane (Cap. 5-6).

• Analisi del Protocollo dal punto di vista della Sicurezza (Cap. 7).

• Un esempio completo (Cap. 8).

• Considerazioni e conclusioni (Cap. 9-10).

Indice

Elenco delle figure

Capitolo 1

LISP: Le Basi

Il Cisco Locator/ID Separation Protocol (LISP) é una nuova architettura di routing. Questa innovativa network-based solution di casa CISCO vanta molteplici peculiaritá in termini di scalabilitá, permettendo ad aziende e service provider di incrementare prestazioni e affidabilitá delle loro reti, riducendo al contempo le complessitá operative derivate dalle tecniche di multi-homing. LISP implementa un nuovo paradigma per l' indirizzamento che consiste nella divisione in due parti dell' IP utente : Endpoint Identifier (EID), che identifica il device host, e il Routing Locator (RLOC) che descrive il modo in cui il device é connesso alla rete. Questo processo di base, che prende il nome di Loc/ID split, permetterebbe di ovviare in parte alle problematiche indotte dalla smisurata crescita della RETE in questi ultimi anni, snellendo sensibilmente la quantitá di informazioni gestite dal sistema di instradamento senza comunque comportare sostanziali modifiche ai sistemi hardware e software esistenti, essendo basato su un particolare schema di map-and-encap. Dichiarato compatibile con il protocollo IPv6, potrebbe secondo la casa madre addirittura portare alcune migliorie in termini di sicurezza della Rete, oltre ad una migliore gestione delle connessioni WAN e al relativo abbassamento dei costi per imprese e gestori.

1.1 Aspettative e Obiettivi

1. Improved routing system scalability by using topologically-aggregated RLOCs.
2. Provider-independence for devices numbered out of the EID space (IP portability).
3. Low-OpEx (Operative Expensive) multi-homing of end-sites with improved traffic engineering.
4. IPv6 transition functionality.
5. IP mobility (EIDs can move without changing - only the RLOC changes).
6. network-based solution . No end-user changes were required.
7. No changes to hosts whatsoever.
8. No new addressing changes to site devices.
9. Very little configuration file changes.
10. Address family-agnostic (IPv4, IPv6 etc).

1.2 In cosa consiste

1.2.1 Locator/ID Separation

Alla base di questa innovazione sta l' assunto che l' IP address sia sovraccaricato. Esso infatti esprime sia l' identificazione del device, che la sua location nella topologia della rete. La parte "Locator" é usata dal sistema di routing, mentre quella "Identity" viene utilizzata da protocolli di piú alto livello come UDP e TCP (upper layer protocols).Questo appunto renderebbe virtualmente impossibile che un unico number space assolva efficacemente

ad entrambi i compiti senza imporre inaccettabili costrizioni (come il renumbering al cambio del provider) sull' uso di quello spazio. La soluzione ipotizzata da CISCO a tal proposito, con la realizzazione di LISP, é proprio la separazione di queste due funzioni attraverso l' uso di differenti numbering spaces per EIDs ed RLOCs. Il ché include inoltre una incrementata scalabilitá del sistema di routing, attraverso una migliore aggregazione degli stessi, che risultano allocati in modo piú congruente con la topologia della rete.

1.2.2 Implementare il Locator/ID Split

Sono stati vagliati due tipi di approccio per realizzare la separazione sopra citata:

- **Address Rewriting:** Questa tecnica, proposta da Dave Clark e Mike O' Dell con il nome di 8+8/GSE, si avvale della disponibiltá di address space capienti come quello tipico del protocollo IPv6. In questa circostanza i 128 bit sono divisi in due parti: i primi 64 esprimono il Routing Locator ("Routing"), mentre i rimanenti 64 bit identificano l' EID. Quando un host emette un pacchetto destinato ad un alro dominio, l' indirizzo sorgente contiene il proprio identificativo (IEEE MAC address) nella seconda parte e uno speciale valore (indenfinito) nel settore RG. Quando altresí un pacchetto destinato a un dominio remoto arriva al router del dominio locale, L' RG sorgente viene inserito (formato un indirizzo completo 128 bit) e il pacchetto ' e indirizzato al dominio remoto. Al suo ingresso, l' RG di destinazione viene riscritto con un altro valore speciale, rendendo impossibile per l' host di conoscere il proprio RG.

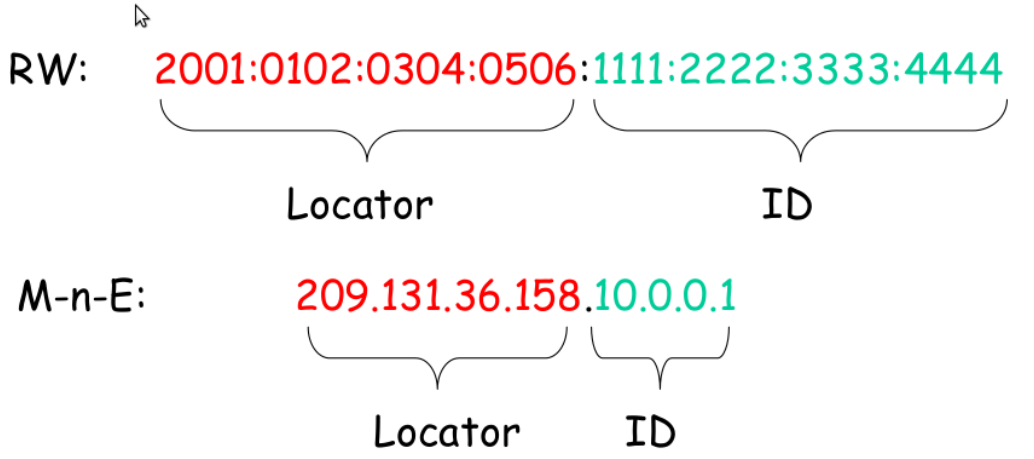

Figura 1.1: Growth of Routing Table

• **Map-n-Ecap:** l' idea generale alla base di questa tecnica, descritta originariamente da Bob Hinden, e Steve Deering, si basa sull' esistenza di due address spaces: una usata senza un dominio (EID) e uno usato per transitare tra i domini (RLOC). Ai routers, a questo punto, il compito di aggregare efficacemente EID space assegnato in maniera non topologica, con un RLOC. Nello schema Map-n-Encap, quando é generato un pacchetto, sia l' indirizzo sorgente che quello di destinazione sono presi dall' EID space. Quando il pacchetto é destinato ad un altro dominio, esso attraversa l' infrastruttura di dominio fino ad un border router che ne mappa la destinazione (dall' EID) in un RLOC space, che verrá poi utilizzato come destinazione dal dominio remoto. Quanto descritto costituisce la fase "Map" dello schema. A questo punto il border router incapsula il pacchetto e setta come destinazione l' Rloc restituito dall' infrastruttura di mapping, concludendo cosí la fase detta "Encap". Entrambi le fasi funzionano attaccando un nuovo header al pacchetto esistente; gli inner header di sorgente e di destinazione sonno contenuti negli EID, gli outer header di sorgente e di destinazione negli RLOCs. Quando un pacchetto

incapsulato arriva al router di destinazione, questo lo decapsula e lo spedisce a destinazione. Questo schema ha la vantaggiosa proprietá di non richiedere modifiche agli Host o all' infrastruttura di rete. Inoltre il modello "Map-n-encap" funziona sia con protocolli IPv4 che IPv6, mantenendo in piú gli indirizzi originari.

1.2.3 Perché quindi la Separazione :

Il livello di indirection (la possibilitá di fare riferimento a un valore usando un nome,un riferimento o un contenitore invece del valore stesso) ci permette di:

- Mantenere fissi ID o locator cambiando il resto.
- Creare separati namespaces che possono avere differenti proprietá di allocazione.

In particolare, la gerarchia di allocazione dell' EID puó seguire una topologia differente rispetto a quella del RLOC :

- Miglior congruenza nella topologia della rete.

Possibilitá di mantenere fissi gli IDs:

- Assegnare indirizzi fissi che non cambiano per host e router rispetto alla posizione.

Possibilitá di cambiare il Locator :

- Now the sites can change providers.
- Now the hosts can move.

Capitolo 2

LISP e il Multihoming

Come largamente ribadito da Fred Backer della CISCO SYSTEM, nella odierna Internet il site multihoming, una network configuration che prevede piú di un service provider ma che non provvede adeguatamente alle comunicazioni in transito tra di essi, é relativamente comune . Secondo le statistiche, ci sarebbero quasi 40.000 Sistemi Autonomi attualmente in rete, di cui circa 5.000 sembrerebbero offrire servizi di transito per uno o piú customers. Per i restanti si ipotizzano quindi principalmente tre possibilitá . Essi potrebbero essere *access networks*, broadband providers che offrono accesso a internet a piccole compagnie e a clientela residenziale ; potrebbero essere *multihomed edge networks*; o potrebbero essere networks che presto o tardi nel futuro effettueranno il multihoming . Ci si aspetterebbe quindi che nel giro di non troppi anni il multihoming coinvolga piú di 50.000 persone in tutto il mondo, diventando sempre piú diffuso, fino ad interessare quasi un quarto della popolazione mondiale . Nel futuro da lui prefigurato ci saranno connessioni per internet TV che si aggiungeranno alle molte altre gestite da molteplici ISPs, tutte su un comune DSL o fibra ottica. Perché quindi questa tendenza al multihoming da parte, soprattutto, della cosi dette edge networks? Le motivazioni possono essere molteplici ; per la situazione sopra descritta sembrerebbe vitale, gli utenti non avrebbero altra scelta ; in un contesto piú generale si potrebbe pensare piuttosto al risultato dei nuovi arrangia-

menti e strategie per raggiungere una buona network reliability attraverso la ridondanza delle reti. I criteri tecnici utilizzati nella selezione di quale potesse essere definito come " IP Next Generation" (IPng), non menzionavano chiaramente il multihoming, pur essendo un caso particolare di flessibilitá e scalabilitá del routing . Quando il protocolo IPv6 fu scelto come eletto, la pratica del multihoming tornó ad essere argomento di discussione, in quanto la comunitá Internet sostenne che questo particolare risultato non fu pienamente raggiunto . Delle varie proposte piú o meno risolutive, tra costi e benefici, nessuna fu selezionata come soluzione definitiva e universalmente accettata. Analizziamone comunque una delle piú importanti:

2.1 BGP Multihoming:

l Border Gateway Protocol (BGP) é uno dei protocolli chiave per ottenere la cosidetta internet connection redundancy tipica delle reti con piú internet service providers (multihomed) . Il multihoming fornisce ridondanza e ottimizzazione della rete selezionando l' ISP che offre il miglior collegamento alla risorsa interessata . Quando si utilizza questo protocollo con piú di un service provider si corre il rischio che il proprio sistema autonomo (AS) diventi un sistema di transito . Questo fa sí che il traffico internet attraversi il proprio AS e potenzialmente occupi tutte le risorse e la banda della CPU del proprio router. IL BGP Multihoming, anche conosciuto come Provider Indipendent Addressing, consiste sostanzialmente in un meccanismo comune nel IPv4 internet ; ciascuna edge network diventa membro di un Regional Internet Registry (RIR) e da questo ottiene un Provider Indipendent (PI) prefix, oppure ottiene un Provider Allocated (PA) prefix da uno dei provider e negozia i contatti con gli altri utilizzando lo stesso prefisso. In ogni caso, esso pubblica il prefisso in BGP e il provider che lo alloca (compreso nel range dei PA) deve trattarlo come un route separato nelle sue routing tables. I vantaggi per le edge network sono facilmente comprensibili e nel caso d grandi organizzazioni il tutto acquisisce importanza ancora maggiore.

I PI Addresses sono in sostanza blocchi di indirizzi assegnati da un pool nel quale non sono associati ad una particolare location nella rete (es. da un particolare ISP), con la conseguenza di avere una aggregazione non topologica per l' intero sistema di routing.

I PA Addresses si trovano in un address block assegnato a un sito da ciascun ISP a cui quel sito si connette. Tipicamente, ciascun blocco diventa sottoblocco del blocco CIDR (Classless Inter-Domain Routing) del service provider ed é aggregato al blocco maggiore prima di essere spedito nella Global Internet. Uno dei problemi piú gravi del protocollo BGP, ma in realtá dell' intera infrastruttura di Internet, deriva dalla crescita della tabella di routing della stessa Internet. Se la tabella di routing globale crescesse fino al punto in cui la sua gestione dovesse superare le capacitá di memoria e di potenza di calcolo dei router meno recenti, questi non sarebbero piú in grado di agire adeguatamente da gateway per le parti di Internet collegate ad essi. Inoltre, cosa forse ancor piú importante, le tabelle di routing piú grandi richiedono tempi piú lunghi per stabilizzarsi dopo una modifica sostanziale nella connettivitá, garantendo nel frattempo solo una connettivitá ridotta, o talvolta assente. La memoria richiesta per archiviare le routing tables, e in alcuni casi i relativi certificati di sicurezza, diventerebbe presto un fattore rilevante nei costi di equipment. Il volume di informazioni che ogni volta andrebbero a riempire le routing tables, la quantitá di energia richiesta dal router in costante pieno regime con la produzione di calore che ne deriverebbe, richiederebbero necessariamente uno switching center termocondizionato. Considerando quindi l' aumento visto dei costi di equipaggiamento richiesti dal transit network, ci si sente autorizzati a pensare che l' operazione sarebbe quantomeno "economicamente meno interessante". Fino al 2001 la tabella di routing globale era in crescita esponenziale e minacciava di dare luogo, col tempo, a una interruzione generalizzata della connettivitá. Nel tentativo di contrastare questa eventualitá,é in corso uno sforzo congiunto degli ISP per mantenere al minimo le dimensioni della tabella di routing globale, attraverso il ricorso ai meccanismi di Classless InterDomain Routing e aggregazione

degli instradamenti. Questi sforzi hanno rallentato la crescita della tabella di routing sino a riportarla a un andamento lineare, allontanando in modo significativo il momento in cui sará necessario sostituire i router piú datati.

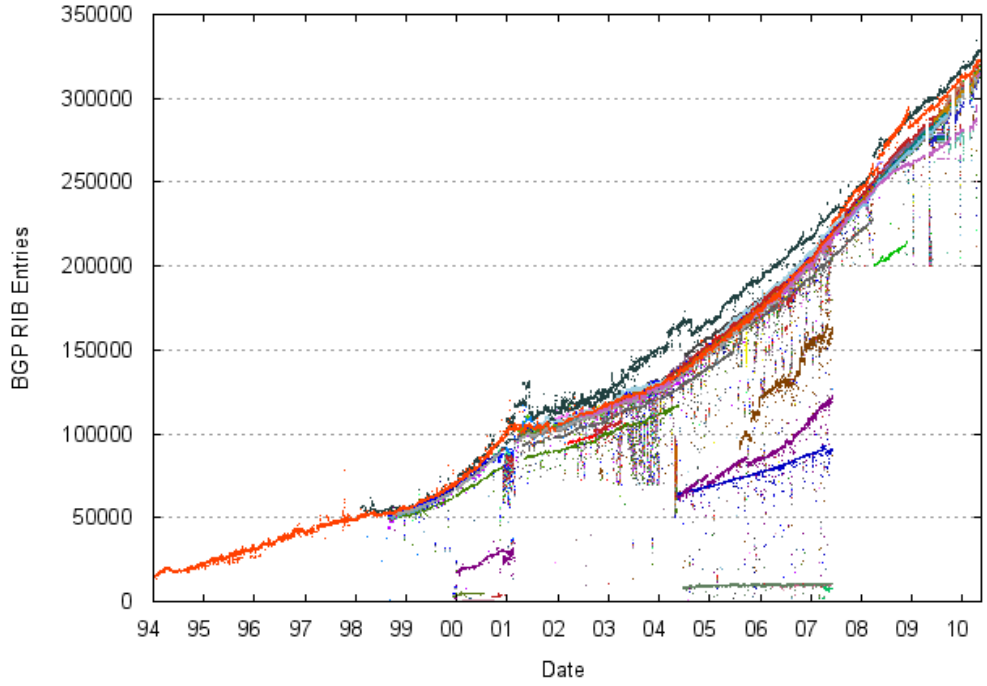

Figura 2.1: Growth of Routing Table

Normalmente, l' IP Multihoming viene implementato da ciascun multi-homed site che acquisisce il suo "globalmente-visibile" prefisso . LISP utilizza esclusivamente blocchi di indirizzi topologicamente assegnati ed aggregati per gli RLOCs, evitando la difficilmente-scalabile pratica descritta sopra . IL progetto LISP si propone di incrementare il site multihoming (per esempio controllando il site ingress senza complessi protocolli), di migliorare l' ISPs multihoming (separando il site addressing dal provider addressing) e di ridurre le dimensioni e le proprietá dinamiche delle core routing tables.

Capitolo 3

L'infrastruttura LISP

3.1 The Locator/Identifier Separation Protocol (LISP):

LISP si propone di risolvere i problemi di scalabilitá di un singolo numbering space per host transport session identification e network routing. E' progettato per essere un semplice, incrementabile, network-based map-n-encap protocol, che implementa la separazione degli indirizzi internet in EIDs ed RLOCs. Essendo un protocollo basato sul map-and-encap, LISP non richiede modifiche agli host stacks, né ai routers esistenti o alle infrastrutture dei database. Ció che essenzialmente avviene é che un EID é mappato ad RLOCs, e poi il pacchetto viene incapsulato con un UDP header che usa l' RLOC addressing. Questo procedimento é anche detto " jack up" siccome l' EID network layer é "jacked up" e l' RLOC addressing é inserito.

Come illustrato dalla figura seguente :

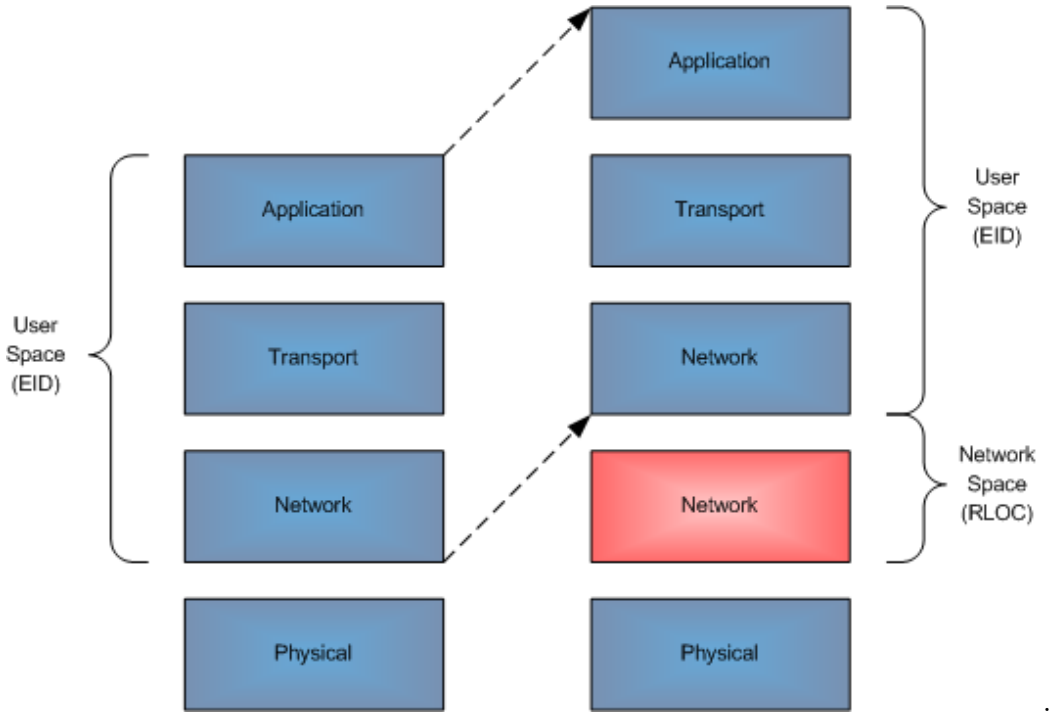

Figura 3.1: LISP Jack-up in Network Layer

3.2 LISP: Elementi funzionali

3.2.1 LISP Name Spaces

- **End-point Identifier (EID) Addresses:** Consistono negli indirizzi IP e nei prefissi che identificano gli end-points . La risoluzione degli EID attraverso i siti LISP é raggiunta tramite l' interpretazione dei mappings EID-to-RLOC .

- **Route Locator (RLOC) Addresses:** Consistono negli indirizzi IP e nei prefissi che identificano i diversi Routers nella rete IP . La risoluzione all' interno degli RLOC spaces é raggiunta tramite i tradizionali metodi di routing .

3.2.2 LISP Site Devices

Le specifiche del protocollo LISP definiscono due principali elementi di rete: un Egress Tunnel Router (ETR) e un Ingress Tunnel Router (ITR). L' ETR riceve il pacchetto IP LISP-encapsuled da internet, da un lato, e spedisce il pacchetto IP decapsulato a siti e sistemi, dall' altro . In particolare, un ETR accetta un IP packet quando il destination address nell' outer IP header é compreso nei suoi propri RLOCs . Il router, a questo punto, elimina l' outer header e instrada il pacchetto in base al successivo IP header trovato . Un LISP Ingress Tunnel Router (ITR) accetta IP packets da siti e sistemi da un lato, e spedisce pacchetti IP LISP-encapsulated attraverso Internet, dall' altro. Nello specifico, un ITR accetta un IP packet con un singolo IP header (piú precisamente un IP packet che non contiene un LISP packet). Il router tratta questo "inner" IP destination address come un EID e realizza un EID-to-RLOC mapping lookup, se necessario (non avendo ancora un EID-to-RLOC mapping per l' EID. A questo punto il router imposta un ' ' outer IP header con uno dei suoi "globally routable" RLOCs nel campo Source Address e il risultato del mapping lookup nel campo Destination Address.

3.3 LISP Infrastructure Devices

- **Map-Server (MS):** Si tratta di uno strumento dell' infrastruttura LISP in cui gli ETRs LISP registrano i loro prefissi EID . I Map-Servers archiviano gli EID prefixes in un database in cui vengono associati agli RLOCs .Tutti i siti LISP, a questo punto, utilizzano il LISP mapping system per effettuare il mapping EID-to-RLOC.

- **Map-Resolver (MR):** Il MR é un device a cui gli ITRs dei siti LISP inviano richieste in forma di Map-Request message per risolvere l' EID-to-RLOC mapping.

L' EID name space é usato all' interno dei LISP sites per l' indirizzamento end-site di host e routers . Questi indirizzi, andranno a far parte dei record dei DNS proprio come avviene oggi. In generale, l' EID namespace non avrá un utilizzo globally routed in questa infrastruttura di trasporto, bensí saranno gli RLOCs ad essere usati per gli indirizzamenti tra LISP routers e core routers (spesso appartenenti agli ISPs)e ad essere globalli router con le stessse modalitá con cui avviene oggi. Gli hosts non avranno informazioni in merito agli RLOCs, i quali non avranno informazioni riguardo agli host.

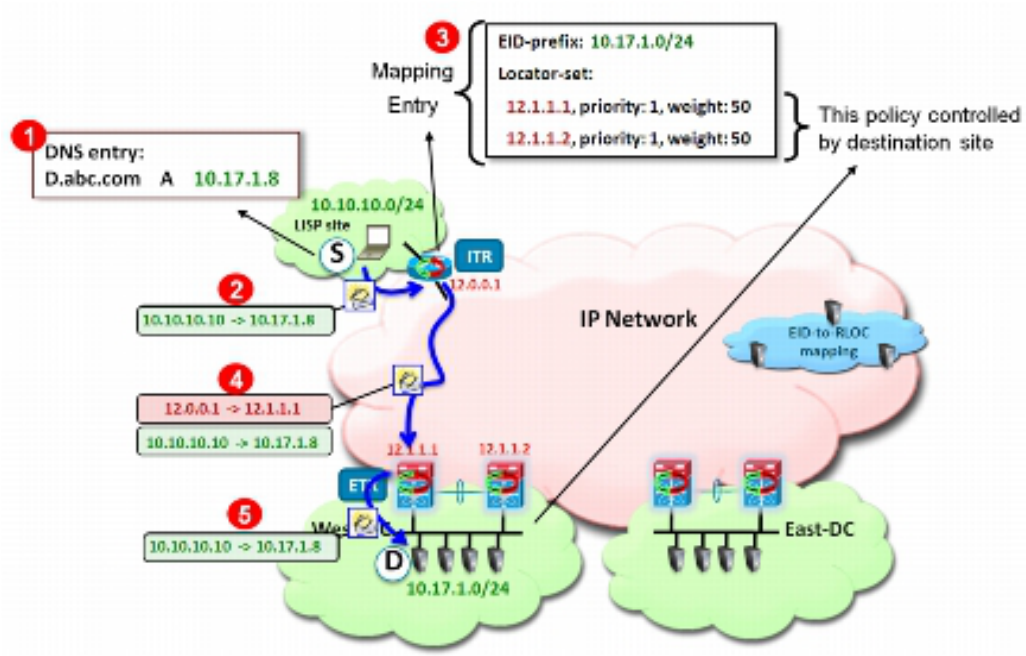

Figura 3.2: Communication between LISP Enabled Sites

1. Il client deposita una richiesta al LISP enabled site remoto, attraverso un DNS in merito all' IP address del Destination server implementato dal LISP enabled Data Center site.

2. Il traffico dati generato dal Client é gestito dal local LISP enabled device (di solito il default gateway del Client). Il LISP device a quel punto attua un lookup per la destinazione (10.17.1.8) nella sua routing table. Se la destinazione é un EID subnet, non sará presente nell' RLOC space e il lookup fallirá, innescando il LISP Control Plane.

3. L' ITR riceve le informazioni di mapping dal mapping Database e con quelle popola la sua map-cache locale. Si noti come la subnet del Destination EID (10.17.1.0/24) é associata agli RLOCs identificativi di entrambi gli ETR device al Data Center LISP enabled site. Inoltre, ciscun inserimento ha associati prioritá e valori di peso, che sono controllati dal destination site per gestire il modo in cui il traffico in entrata sará ricevuto dall' infrastruttura di trasporto. La prioritá é usata per determinare se entrambi gli ETR device possono essere usati per ricevere traffico LISP incapsulato desinato ad una EID subnet locale. Il valore di peso permette di modulare le quantitá di traffico ricevute da ciascun ETR in uno scenario di load-balancing (metodo con il quale le richieste di connessione ad un sito vengono deviate, fra server diversi che mantengono lo stesso sito, a quello che in quel momento presenta un quantitativo inferiore di traffico); questo parametro entra in gioco quando ci si trova in una condizione di pari livello di Prioritá per gli ETRs locali.

4. Nella fase di Data Plane, l' ITR attua una encapsulation del traffico IP originale e lo dirigge all' infrastruttura di trasporto, destinandolo ad uno degli RLOCs degli ETRs Data Center.

5. L' ETR riceve quindi il pacchetto, lo decapsula, e lo instrada al destination EID.

- **Proxy ITR (PITR):** Un Proxy ITR é un device il cui scopo é quello di permettere la connettivitá tra non-LISP sites and LISP sites accettando traffico non-LISP destinato a LISP sites e incapsulandolo prima di presentarlo agli ETR devices implementati al LISP site.

- **Proxy ETR (PETR):** Un PETR é un device infrastrutturale che permette agli EIDs di comunicare con successo con devices situati in un non-LISP site.

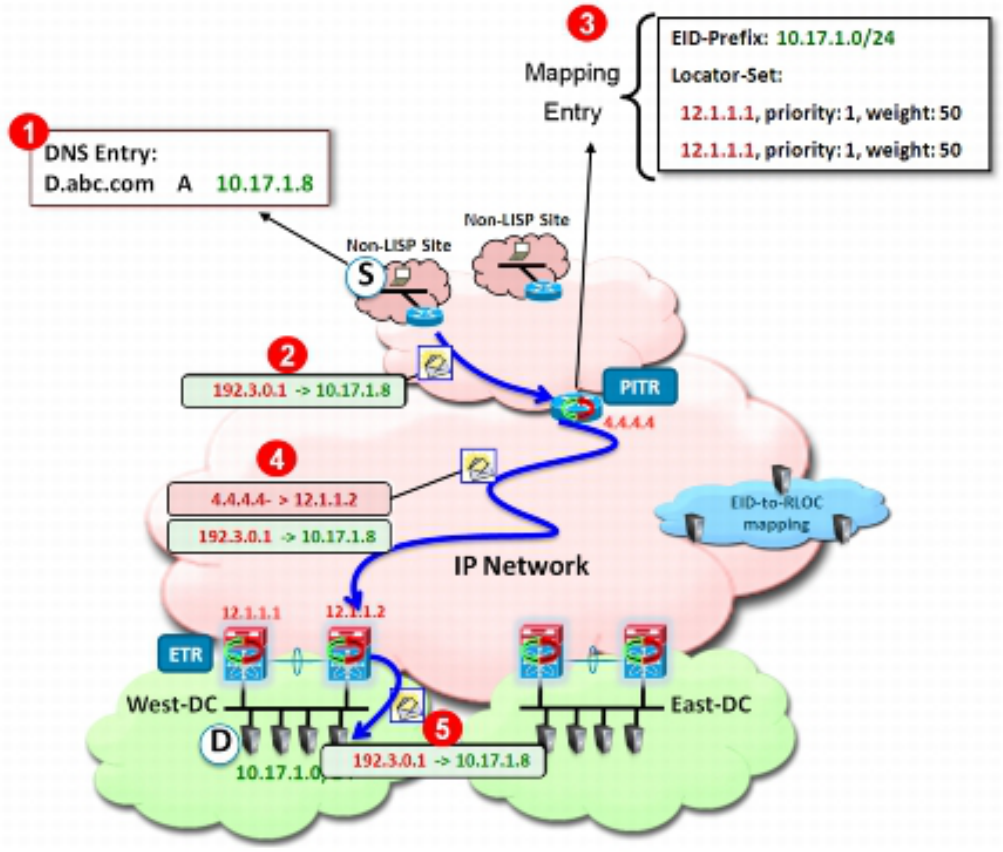

Figura 3.3: Communication between non-LISP Enabled Sites and LISP Enabled Sites

Capitolo 4

Tunneling

4.1 Introduzione

Uno dei punti chiave di questo protocollo é l' assunto che l' end-system mantenga per la maggior parte le stesse procedure operative di oggi. L' IP address che un host (end-system) utilizza per tracciare le connessioni e per spedire e ricevere pacchetti non cambia. Nella terminologia LISP questi sono conosciuti come EIDs. I routers continueranno a instradare pacchetti basati su IP Destination Address; quando un pacchetto LISP-encapsulated viene elaborato, questi indirizzi vengono riferiti come RLOCs. La maggior parte dei Routers continueranno ad operare come fanno oggi instradando i pacchetti. Per quelli che sono connessi agli end-systems o xTR, i destination addresses saranno gli EIDs. Per i Router tra gli ITR e gli ETR, gli indirizzi saranno gli RLOCs . Lo schema LISP introduce i " tunnel routers", i quali attaccano LISP headers in fase di spedizione, e li rimuovono in fase di ricezione. Gli indirizzi IP in questi " outer" LISP headers sono gli RLOCs. Gli ITR effettuano l' EID-to-RLOC lookup cosi da determinare il percorso di routing per l' ETR, che ha l' RLOC come uno dei suoi IP addresses.

4.2 Concetti di Base

- Gli End-systems spediscono solamente ad indirizzi che sono anche EIDs. Loro non sanno che gli EIDs sono mappati con RLOCs, ipotizzano solamente che i pacchetti sono destinati ai routers LISP, i quali li instradano alle corrette destinazioni finali.

- Gli EIDs sono sempre indirizzi IP assegnati agli hosts.

- Gli RLOCs sono sempre indirizzi IP assegnati ai Routers, preferibilmente indirizzi topologicamente orientati dai CIDR blocks dei Providers.

- Quando il Router é la sorgente del pacchetto, esso puó usare come source address sia un EID che un RLOC. Quando invece si comporta da host (Telnet, SSH connections) puó usare un EID esplicitamente assegnato a questo proposito. Un EID che identifica un router non deve mai essere usato come RLOC poiché esso sará routabile solo localmente per scopi limitati a quel sito. Un buon esempio di comportamento ibrido puó essere una BGP configuration in cui il router utilizza il suo EID locale per terminare sessioni iBGP e il suo RLOC per intraprendere sessioni eBGP.

- Gli EIDs non sono pensati per essere utilizzati globalmente in comunicazioni "end-to-end". Se proprio non é presente un mapping EID-to-RLOC, allora é pensabile utilizzarli per comunicazioni esclusivamente intra-site.

- Gli EID-prefixes sono assegnati gerarchicamente ed in maniera da essere ottimizzati per convenienza amministrativa e per migliorare la scalabilitá del l' EID-to-RLOC mapping database.

- Quando un tunneling ricorsivo viene implementato, le specifiche raccomandano che non piú di due LISP headers siano attaccati al pacchetto. In questo modo si rischia un eccessivo overhead del pacchetto e possibili loops in fase di encapsulation . Si presume infatti che due headers

siano sufficienti nel caso in cui il primo header sia ataccato dall' ITR e il secondo dal TE-ITR.

4.3 Packet flow sequence

Nella figura seguente un esempio di trasmissione di pacchetti:

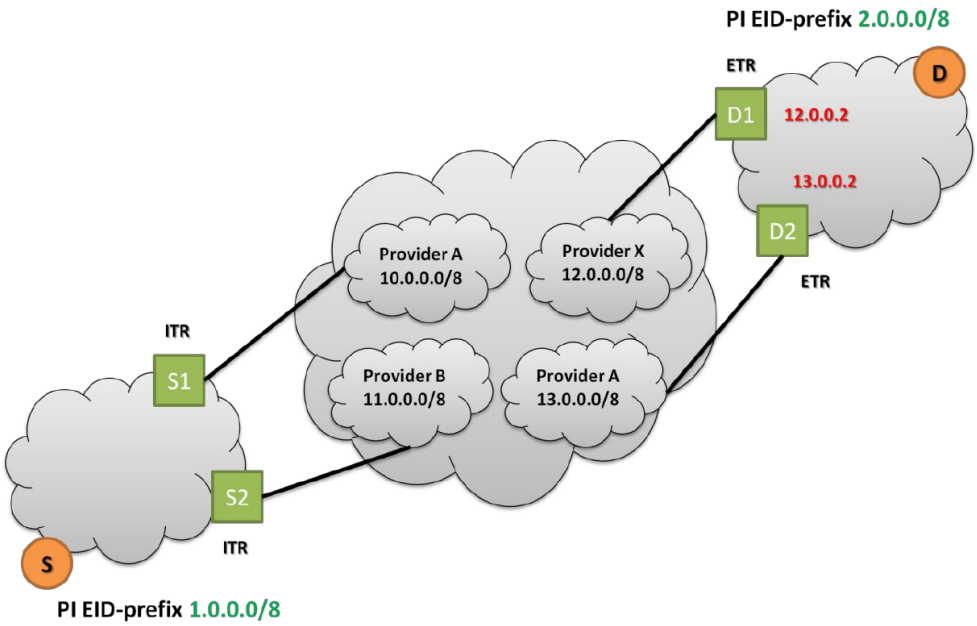

Figure 3. Transmission of LIPS packet

Figura 4.1: Trasmission of LISP Packet

- La Sorgente S cerca di trasmettere un pacchetto alla Destinazione D, con la quale apre una connessione TCP effettuando quindi un DNS lookup. Dopo la ricezione degli indirizzi dal DNS, la Sorgente utilizza questo indirizzo come Destination EID, e il local assigned IP address come Source EID. Un pacchetto IPv4 o IPv6 é costituito usando gli EIDs nei rispettivi header e spedendo il tutto al default router.

- Il default router S1 é configurato come ITR e deve essere in grado di mappare il Destination EID in un RLOC dell' ETR al sito di destina-

zione. L' ITR attacca un LISP header al pacchetto con uno dei suoi RLOCs come sorgente nell' indirizzo IPv4/IPv6. L' indirizzo EID di destinazione dell' originale packet header viene utilizzato come IPv4/IPv6 di destinazione nell' header appena attaccato. Il pacchetto viene quindi spedito con l' outer destination address settato all' EID finché non verrá ottenuto un mapping EID-to-RLOC.

- A livello dell' ETR, il LISP header viene rimosso e il pacchetto viene instradato dal Router, che effettuerá il lookup del Destination EID nel suo EID-to-RLOC database e infine spedirá il pacchetto in maniera appropriata.

- Un Map-Reply message é configurato e spedito nella giusta direzione all' RLOC del sito sorgente . Alla ricezione del Map-Reply message, l' ITR Sorgente metterá in cache l' informazione, dopo aver verificato la format validity del messaggio.

- I pacchetti seguenti, da sorgente a destinazione, presenteranno gli RLOCs dell ETR come destination address nei LISP header attaccati.

- L' ETR riceverá questi pacchetti direttamente, rimuoverá il LISP header e li instraderá all' end-system preposto.

- Per eliminare il mapping lookup in direzione opposta, l' ETR puó costituire una cache entry per gli RLOCs dell' ITR sorgente.

4.4 Tunneling Details

Considerando che all' IP packet saranno attaccati ulteriori tunnel headers, le dimensioni di questo potrebbero superare l' MTU (maximum transmission unit) di ogni link attraversato nel percorso dall' ITR all' ETR. Se, per esempio, un IPv4 packet risultasse di dimensioni maggiori dell' MTU, questo non verrá frammentato dall' ITR in fase di encapsulate, bensí sará tralasciato, restituendo un ICMP Too Big message alla sorgente. Basandosi su informazioni informali riguardanti la maggior parte degli ISPs in circolazione, sembra che un buon numero di questi sia in grado di gestire MTU di almeno 4770 bytes. Per quanto riguarda gli altri, in termini di data rate, numero di host interessati o ogni altro criterio utilizzato, sembra siano in numero trascurabilmente minore. A questo proposito, comunque, lo sviluppo di LISP includerá una raccolta di dati durante la sua fase pilota per verificare o smentire quanto assunto in termini di MTU disponibili. Nel primo caso risulterebbe relativamente economico aggiornare o modificare le poche transit network inadeguate a supportare MTUs di dimensioni maggiori o ad usare meccanismi preesistenti per gestire pacchetti "troppo grandi". Ottimisticamente LISP non prevede ancora meccanismi aggiuntivi per implementare la frammentazione e il riassemblaggio in caso di MTU transit links limitati ; ma se risultasse vero il contrario sarebbe necessario modificare il protocollo di standardizzazione per aggiungere i supporti adeguati, che sono comunque giá stati ipotizzati e proposti.

4.4.1 LISP IPv4 in IPv4 Header Format

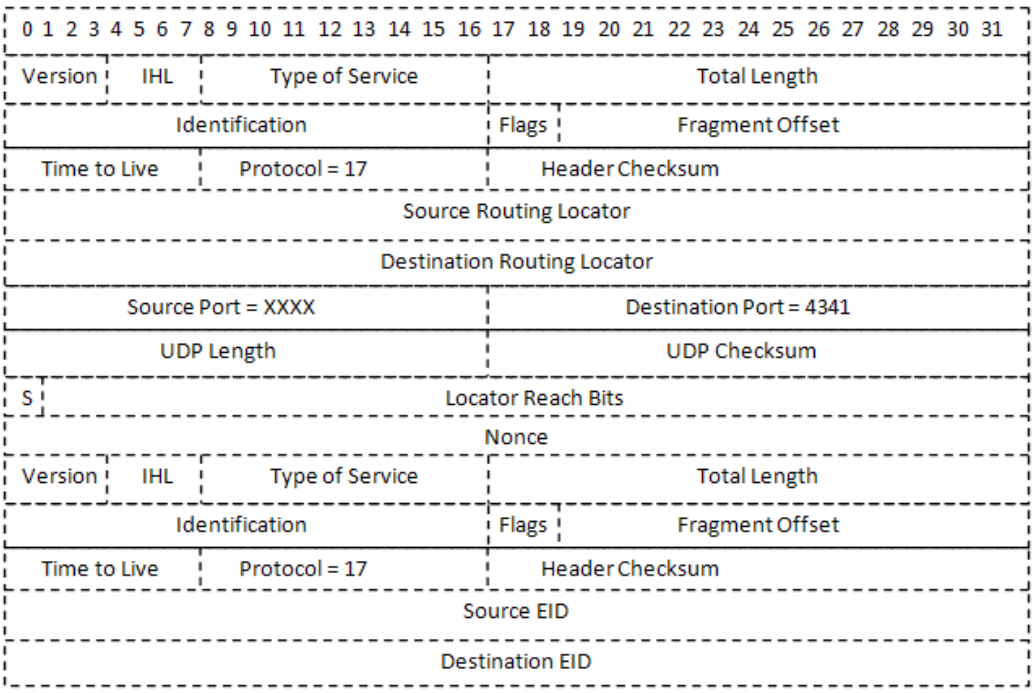

Figura 4.2: LISP IPv4 Header Format

4.4.2 LISP IPv6-in-IPv6 Header Format

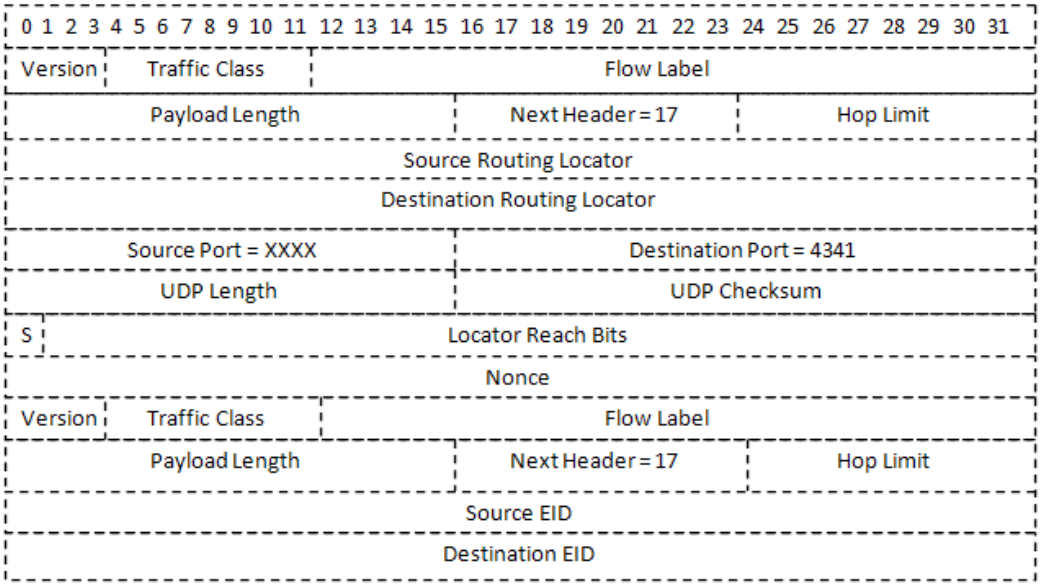

Figura 4.3: LISP IPv6 Header Format

Capitolo 5

Data-Plane

5.1 LISP Data-Plane Operation

Quando un host, in un dominio LISP-compatibile, emette un pacchetto, inserisce il suo EID nel packet source address, e l' EID del corrispondente host nel suo destination address (si ricorda che gli hosts tipicamente effettuano il lookup degli EIDs nel Domain Name System). Se la destinazione del pacchetto trasmesso si trova in un altro dominio, questo attraversa l' infrastruttura sorgente verso uno dei suoi ITRs, il quale mappa l' EID di destinazione in un RLOC che corrisponde ad un ETR che si trova nel dominio di destinazione, o ad un proxy che indirizza allo stesso. L' ITR, a questo punto, incapsula il pacchetto settando il destination address all RLOC dell' ETR restituito dall' infrastruttura di mapping, oppure secondo una configurazione statica. Come piú volte assunto in precedenza, LISP é per progettazione address family-agnostic, e come tale puó essere utilizzato in entrambi i piú diffusi protocolli IP (IPv4 e IPv6).

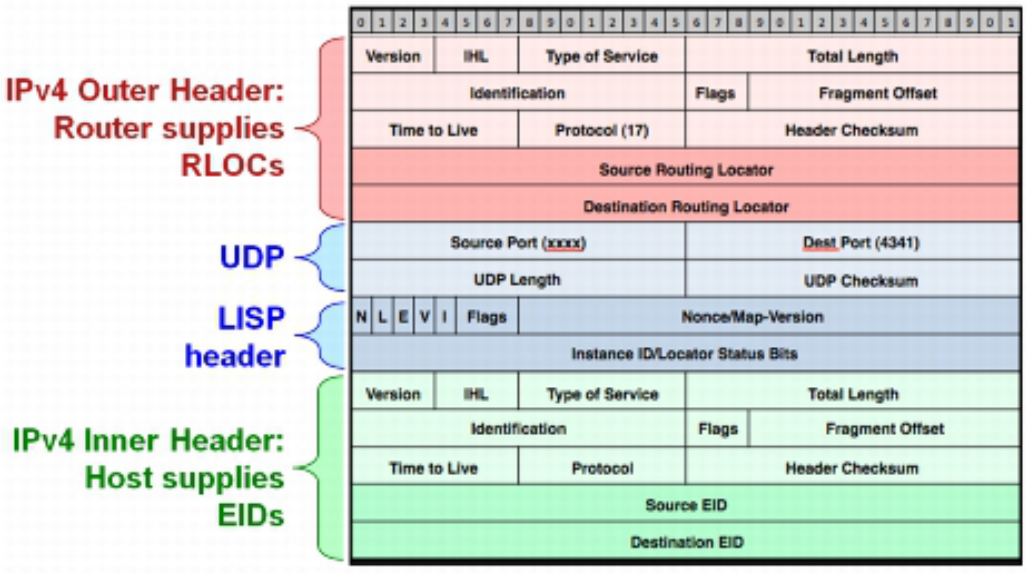

Figura 5.1: Lisp IPv4 in IPv4 encapsulation

Quando un pacchetto arriva al Destination ETR, questo lo decapsula e lo spedisce a desinazione.

Le specifiche del protocollo LISP definiscono tre tipi di pacchetti, designati a supportare un EID-to-RLOC mapping system:

Definiti nel modo seguente:

- Il primo tipo, il *Data Probe*, é un pacchetto di dati che un ITR puó mandare al mapping system per sondare il mapping; l' ETR accreditato risponderá con un Map-Reply message al ricevimento del pacchetto.

  In questo caso l' ETR capirá che si tratta di un pacchetto *Data Probe* in quanto noterá che l' inner Destination Address (DA) é stato copiato come outer DA dall ' ITR (sará in pratica un EID).

- Il secondo tipo di pacchetto usato per supportare il mapping system é il Map-Request. Questo tipo di messaggio puó essere usato da un ITR per richiedere al mapping system un particolare EID-to-RLOC mapping. Come nel caso precedente l' authoritative ETR risponderá con un Map-Reply message.

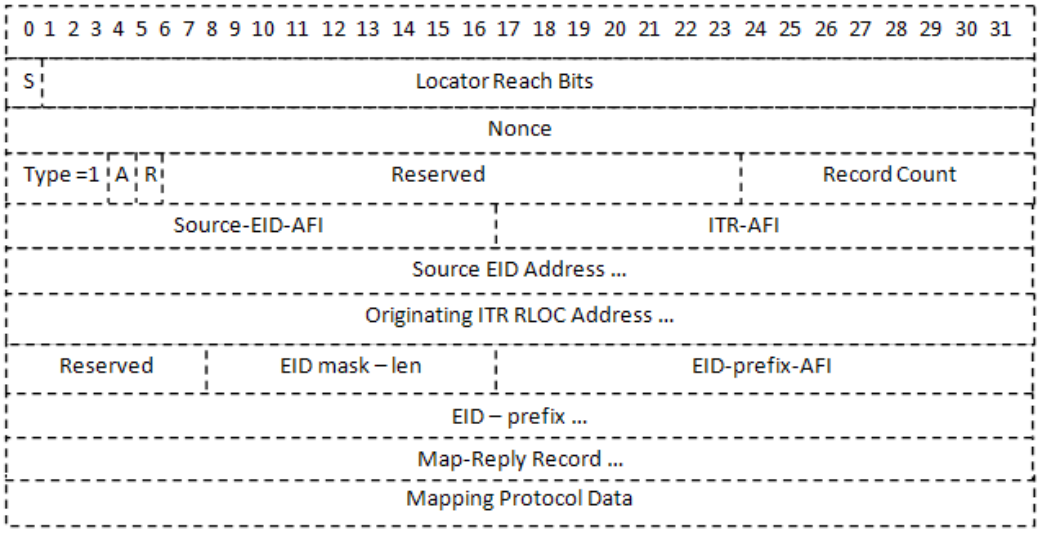

Figura 5.2: Map-Request Message Format

- Il terzo tipo di pacchetto é infine il Map-Reply. Un ETR emette questo tipo di messaggio principalmente come risposta nelle due circostanze sopra descritte.

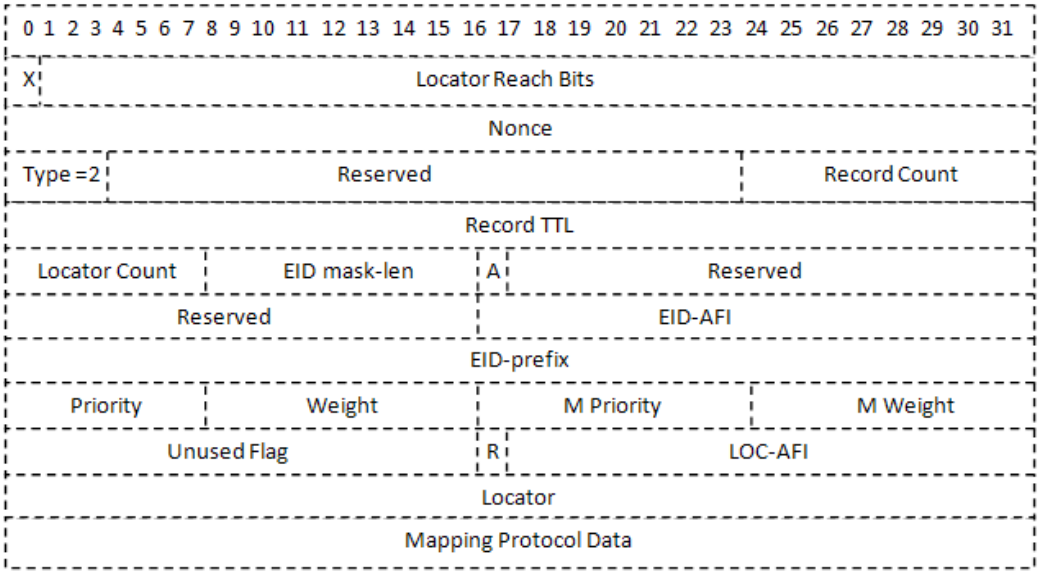

Figura 5.3: Map-Reply Message Format

Capitolo 6

Control Plane

6.1 LISP control Plane

Nella figura 6.1 viene spiegato LISP control Plane:

1. Gli ETRs registrano con il Map Server le subnet EID che sono locally defined per le quali sono authoritative. In questo esempio l' EID subnet é 10.17.1.0/24. Messaggi di map-registration sono quindi spediti ogni 60 secondi da ciascun ETR.

2. potizzando che non sia disponibile una local map-cache entry, quando un Client vuole stabilire una comunicazione con un Data Center EID, viene spedita una Map-Request dall' ITR remoto al Map-Resolver, il quale inoltra il messaggio al Map Server.

    - NOTA: Le funzionalitá di Map-Server e Map-Resolver possono essere abilitate entrambe sullo stesso device.

3. Il Map Server inoltra la Map-Request originale all' ETR che per ultimo ha registrato l' EID subnet . In questo caso si tratta dell' ETR con locator 12.1.1.2.

4. L' ETR spedisce all' ITR un Map-Reply contenente la mapping information richiesta.

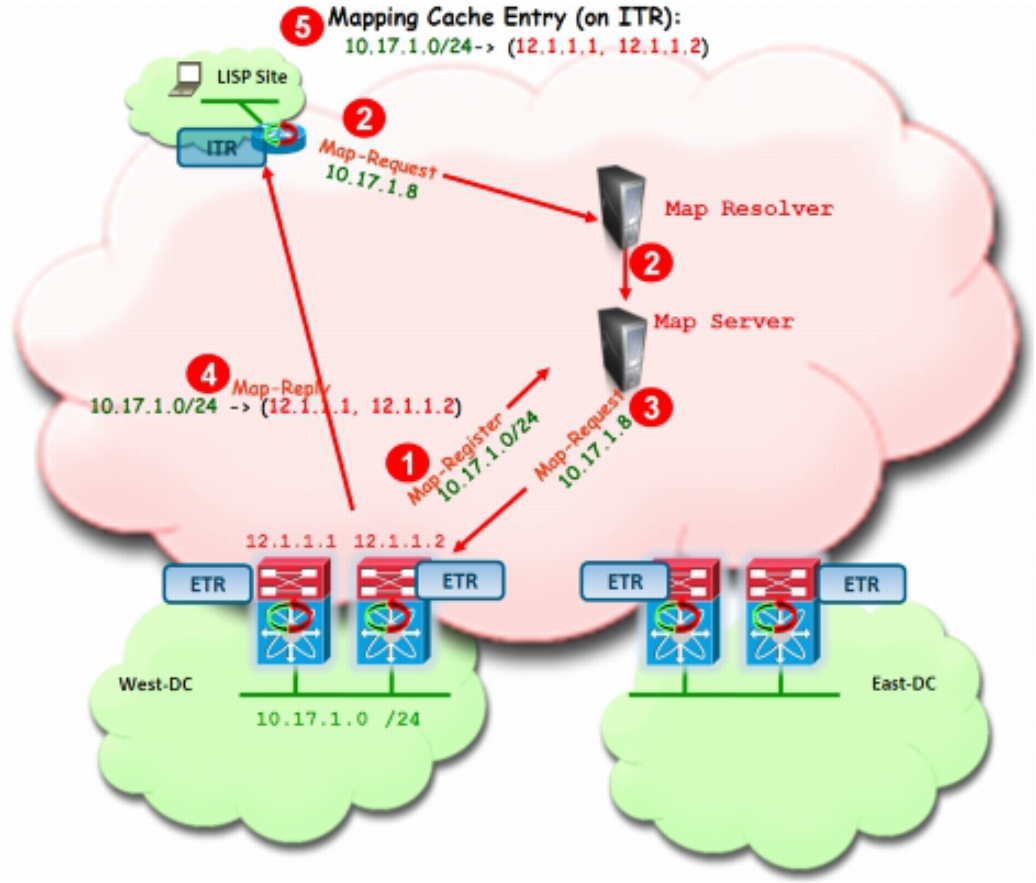

Figura 6.1: Control Plane

5. L' ITR inserisce la mapping information nella sua local map-cache e inizia ad incapsulare traffico dati verso il Data Center EID.

Entrambi i processi, di map-and-encap e address rewriting, concorrono a realizzare un livello aggiuntivo di indirection nell' architettura di addressing che contribuisce a rendere il routing system ragionevolmente scabile. Siccome i pacchetti sono originati con un EID nel campo Destination Address e gli EIDs non sono in generale routabili nella global internet, il destination EID deve essere mappato in un RLOC per poter spedire il pacchetto ad un altro dominio (che implica di attraversare internet). Nel caso di map-and-encap si realizza una traslazione diretta : un EID viene mappato in un RLOC. La situazione é sostanzialmente differente per quanto concerne il processo di rewriting ; in generale secondo questo schema é necessario stimare l' intero Destination Address (che normalmente si troverebbe come DNS), richiedendo di determinare l' RG (Routing Group) sorgente quando si riscrive il source address al dominio finale. In ognuno dei modelli "Loc/ID split", é richiesto un sistema di mapping EID-to-RLOC che lo renda ragionevolmente scalabile e operativamente attuabile. Esistono tre importanti parametri da rispettare quando si progetta un' architettura di mapping service :la cadenza di update del mapping database, le condizioni richieste per essere accettato dal mapping service, e il periodo di latenza dovuto al database lookup. Le proprietá di scalabilitá del database sono frequentemente condizionate dalla ricerca del giusto compromesso tra questi tre fattori.

6.1.1 LISP-Alternative-Topology

L' idea alla base di LISP-Alternative-Topology (LISP-ALT) consiste nel costruire una topologia logica alternativa per gestire il mapping EID-to-RLOC di LISP. Questa logical topology utilizza tecnologia e funzioni pre-esistenti, in particolare il BGP (Border Gateway Protocol) e la sua estensione multiprotocollo, unitamente al Generic Routing Encapsulation (GRE) Protocol, per creare una overlay network di devices che implementano escusivamente prefissi EID . Come nel caso del LISP Data Plane, un importante design goal della LISP-ALT é quello di minimizzare il numero di modifiche richieste all' hardware e al software esistenti per implementare il mapping system . Essa infatti non richiede modifiche di alcun genere né al BGP, né al GRE. Si noti, che LISP-ALT costituisce quella che viene definita una hybrid push-pull architecture. Aggregati prefissi EIDs, infatti, sono "pushed" verso i LISP-ALT routers e, in alternativa, verso gli ITRs (i quali possono scegliere se ricevere "aggregated information" o semplicemente utilizzare un default mapping). Specifici mappings EID-to-RLOC sono "pulled" dagli ITRs come Map Requests o Data Probes, i quali vengono instradati attraverso l' alternate topology e restituiti nelle Map Replies generate dagli ETRs. Il principio alla base di LISP-ALT, in aggiunta, consiste nell' utilizzare il BGP unitamente al GRE per ottenere l' accessibilitá richiesta per instradare Data Probes, Map Requests e Map Replies attraverso la alternate topology. L' ALT-RIB (Routing Information Base) comprende i prefissi EID e i successivi passi associati. I routers LISP-ALT comunicano con gli altri tramite External BGP (eBGP) per propagare le informazioni di aggiornamento sui prefissi EIDs, che sono acquisite, sempre tramite connessioni eBGP, dagli authoritative ETRs o da configurazione. Gli ITRs possono inoltre comunicare tramite Ebgp con uno o piú routers LISP-ALT per instradare pacchetti Data Probe e Map Requests. In sintesi, LISP-ALT utilizza BGP per propagare informazioni di disponibilitá dei prefissi EIDs usate da ITRs ed ETRs per inviare Map Requests, Map Repleies e Data Probe. Questa "disponibilitá" viene trasmessa come IPv4 o IPv6 Network Layer Reachability Information

(NLRI) senza alcuna modifica, poiché l' EID space presenta la stessa sintassi di IPv4 e IPv6. I routers LISP-ALT comunicano l' uno con l' altro tramite connessioni eBGP, formando overlay network, aggregano EID prefixes e instradano i tre tipi di messaggi.

Capitolo 7

Sicurezza

7.1 Panoramica

Il Locator/ID Separation Protocol (LISP) é un' architettura di routing di nuova generazione che é stata sviluppata dalla CISCO e dall' IETF, la quale introduce un nuovo modello per l' IP addressing che crea un livello di indirection usando due namespaces : gli endpoint identifiers (EIDs), che sono assegnati agli end hosts, e i routing locators (RLOCs), che sono assegnati ai devices (principalmente routers) che implementano il global routing system. LISP inoltre gestisce separatamente le funzioni di data-plane (instradamento del cosidetto user traffic) e quelle di control-plane (l' insieme delle operazioni di protocollo e routing). Queste features introducono nelle odierne architetture di routing molti moglioramenti, come ad esempio incrementare la scalabilitá del routing, semplificare il site multihoming e l' ingress traffic engineering, l' IP portability, l' IP mobility, e la coesistenza dei protocolli IP Version 4 e Version 6. Dal punto di vista della sicurezza, lo sviluppo e la diffusione di ogni nuovo protocollo richiede che si affronti approfonditamente questa problematica ; e in questo LISP ha tenuto in considerazione fin da principio.

Tre in particolare sono state le aree prese in esame:

- La sicurezza inerente al Protocollo
- L' impatto della sua diffusione sulle reti esistenti
- Le nuove funzioni di sicurezza introdotte dal Protocollo

7.2 Sicurezza Inerente al Protocollo

Fin dalla fase di sviluppo di LISP, le valutazioni sulla sicurezza si sono evolute a lungo, considerando le necessitá e le specifiche richieste degli altri protocolli in vigore. Tenendo in considerazione la linea sottile che divide un livello "adeguato" di sicurezza che la realistica diffusione degli indirizzi concerne, e un accesso di sicurezza, che ne preclude l' adozione, lo sviluppo di questo protocollo si é impegnato ad assicurare che Internet "con LISP" non sará meno sicura di Internet stessa. Nuovi meccanismi di sicurezza, che ottemperano a specifiche richieste operative, sono in continua individuazione ed evoluzione; quanto LISP stesso .

Attualmente il Protocollo include una Map-Register authentication, nonce per Map-Request e Map-Reply (contrazione delle parole inglesi number used once: numeri casuali o pseudo casuali utilizzati spesso nei protocolli di autenticazione per assicurare che i dati scambiati nelle vecchie comunicazioni non possano essere utilizzati in attacchi di tipo Replay Attack), e altri meccanismi interni come l' EID source checks e i control-message rate limits.

Unitamente, il protocollo é stato sviluppato per poter accogliere ulteriori miglioramenti da altri meccanismi di sicurezza, come il supporto di una full PKI (Public Key Infrastructure : insieme di processi e mezzi tecnologici che consentono a terze parti fidate di verificare e/o farsi garanti dell' identittá di un utente oltre che di associarvi una chiave pubblica) internamente al Control Plane; o l' aggiunta dell' IP Security (standard per reti a pacchetto che si prefigge di ottenere connessioni sicure su reti IP attraverso funzionalitá di autenticazione, cifratura e controllo di integritá dei paccchetti) per

authentication ed encryption dei LISP data-plane and control-plane packets, come richiesto per venire incontro alle necessitá di sicurezza.

7.3 Impatto della Diffusione del Protocollo LISP

La diffusione di LISP dovrebbe essere semplice e lineare. Per quello che riguarda la sicurezza sono stati individuati due pricipali aspetti che necessitano di essere gestiti. Per primo, i firewall esistenti dovranno essere modificati per permettere il LISP control-plane and data-plane packets. In seconda istanza, bisogna considerare che LISP implica l' encapsulation dello user traffic. Durante il networking, gli attuali meccanismi di sicurezza, come firewall o altri sistemi di prevenzione delle intrusioni, dovranno essere in grado di agire sugli user payloads (cargo dati oggetto della trasmissione) nei LISP header, operando ad esempio ispezioni approfondite dei pacchetti. Questi requisiti, in fondo, non sono diversi da quelli richiesti per ogni altro meccanismo di tunnel and encapsulation presente oggi, come per esempio GRE (Generic Routing Encapsulation) oppure MPLS (Multiprotocol Label Switching). Come si puó vedere dalla figura alla pagina seguente, l' outer header punta alla location topologica, l' inner header punta all' end host e puó essere sottoposto a policy di sicurezza. A livello dei LISP site, non sono richieste modifiche visto che l' host IP rimarrá invariato.

Siccome i LISP EIDs (host IP addresses)non cambiano, l' implementazione delle policy di sicurezza puó essere semplificata. Come illustrato in figura 7.2, nel modello LISP, le firewall policies per il disaster-recovery data center possono essere identiche a quelle per il primary data center firewall, poiché i servers avranno identici IP addresses. Questa feature riduce contemporaneamente i costi operativi (OpEx:Operative Expensive) e la possibilitá di errori di configurazione .

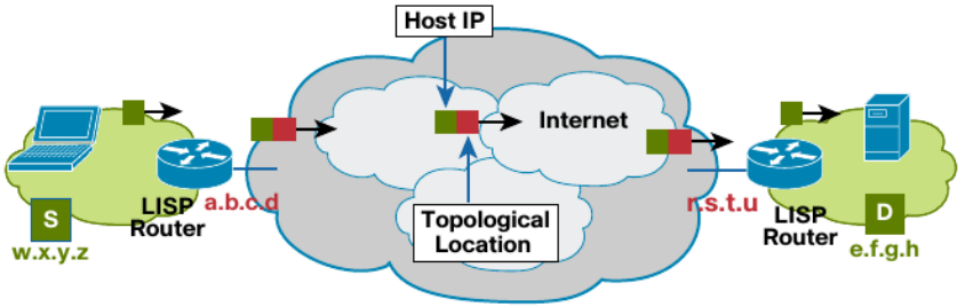

Figura 7.1: LISP Encapsulation Concepts

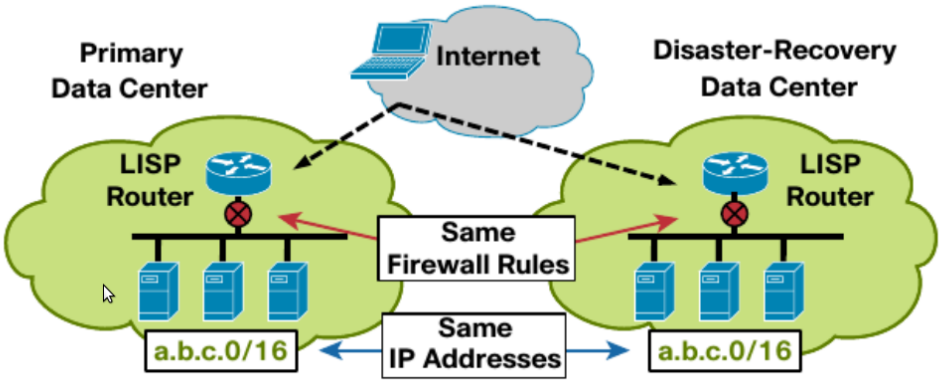

Figura 7.2: Unified Security Polocies Based on End Hosts

7.4 Nuove Funzioni di Sicurezza Introdotte dal Protocollo

Considerando il livello di indirection creato tra gli end hosts e le locations, LISP rende possibile l' introduzione di nuove security features non ancora disponibili nelle architetture di routing attualmente diffuse. Uno di benefici auspicati era gia evidente in Figura 7.2. Non imponendo infatti modifiche agli host IP addresses, il policy enforcement puó essere basato sull' identitá, piú che sulla location. Come illustrato in Figura 7.3, nuovi ulteriori meccanismi di policy enforcement risultano ora possibili. Le LISP ingress

traffic-engineering control policies possono essere usate come meccanismo di "push-back" contro i Distributed Denial-of-Service (DDoS) attacks con lo scopo di causare un drop dell' offending traffic dall' encapsulator, oppure di redirigere quel traffico ad uno scrubbing center. Questo tipo di attacchi sono considerati come un congestion-control problem, ma siccome la congestione in questo caso viene causata da malicious hosts che non obbediscono al tradizionale end-to-end congestion control, il problema deve essere gestito dai routers. Funzionalmente ciascun router ha il compito di individuare i pacchetti che probabilmente appartengono a questo tipo di attacco ed effettuare un drop di questi (da qui il nome di pushback) per fare in modo che le proprie risorse siano utilizzate per gestire il solo traffico legittimato.

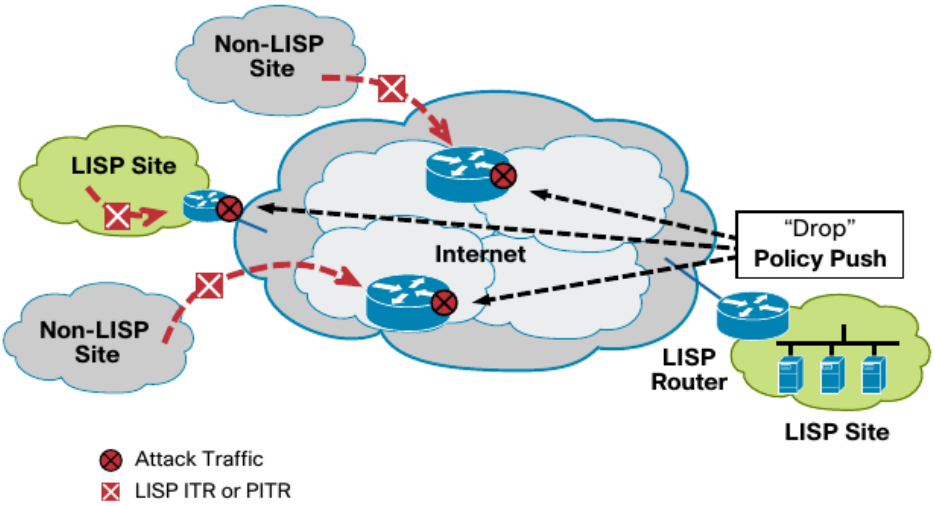

Figura 7.3: LISP Ingress Traffic Engineering a Push-Back Mechanism

LISP inoltre aiuta a facilitare la diffusione di VPNs altamente scalabili. Il suo out-of-band control plane, insieme alla capacitá di dynamic encapsulation e a quelle di virtualizzazione integrata, sono il supporto ideale per questo tipo di reti, come evidenziato dalla figura seguente.

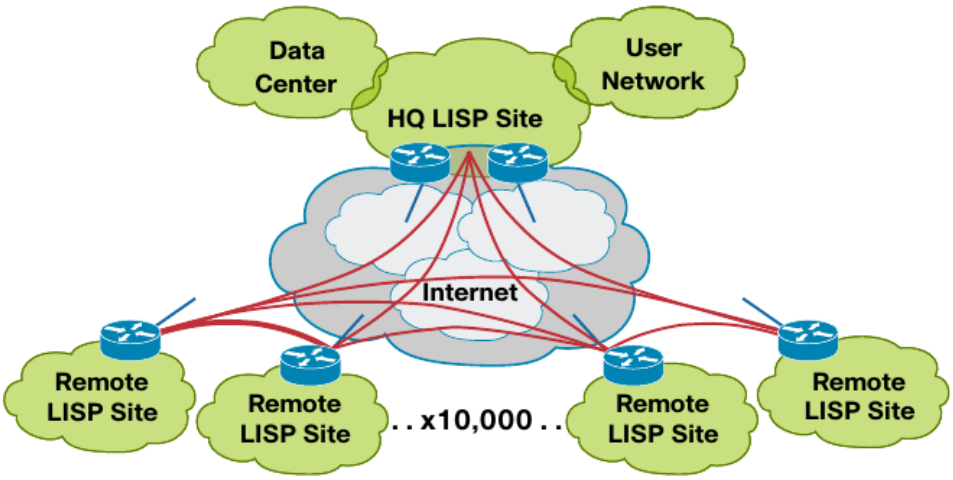

Figura 7.4: LISP and Highly Scalable VPNs

Capitolo 8

Un esempio Completo

8.1 Un giorno nella vita di un pacchetto LISP

Quando in un dominio LISP-compatibile un host vuole spedire un pacchetto, prima effettua un look up dell' EID corrispondente nel DNS, successivamente inserisce il proprio EID nel Source Address e l' EID del corrispondente host nel suo Destination Address ; se la destinazione del pacchetto in questione si trova in un altro dominio, questo attraversa la Source domain infrastructure verso uno degli ITRs del dominio.

A questo punto, se nella cache dell' ITR é gia presente un mapping EID-to-RLOC per il Destination EID, setta il Destination RLOC nell' outer header (incapsulato) con l' RLOC in cache, e il Source RLOC con il proprio RLOC (si noti che l' inner header avrá come sorgente l' EID del Source host e come destinazione il Destination EID. Il pacchetto sará quindi spedito, attraverso Internet, all' ETR indicato nel Destination RLOC, che lo decapsulerá e lo invierá al Destination EID.

Se invece l' ITR non ha nella cache un mapping EID-to-RLOC per il Destination EID, esso incapsula il pacchetto in un LISP header in cui il Destination Address sará uguale al Destination Address dell' inner header, e quindi all' EID del Destination host. Questo pacchetto é di tipo Data Probe, ed é spedito attraverso una LISP-ALT topology al LISP-ALT router che é "au-

thoritative" per il mapping EID-to-RLOC. Quando il corrispondente ETR riceve il Data Probe Packet, lo decapsula e lo spedisce al Destination EID, inviando una Map Reply al Source ITR cosicché i pacchetti seguenti saranno spediti di default attraverso Internet (in opposizione alla LISP-ALT overlay network). Questa transazione domanda/risposta é necessaria esclusivamente per il primo pacchetto spedito tra sites: tutti i pacchetti successivi saranno instradati LISP-encapsuled direttamente tra ITR e ETR, ed in particolare senza passare dalla LISP-ALT topology.

Infine, si noti che l' ITR é anche in grado di precaricare nella propria cache i mapping per le destinazioni piú popolari usando il Map Request message, evitando il Data Probe packet e la conseguente latenza associata. Consideriamo ad esempio lo scenario presentato nella figura seguente. In questo caso, una sorgente S con EID 1.0.0.1 vuole instradare un pacchetto alla destinazione D il cui EID é 2.0.0.2 . Il pacchetto in questione arriva all' ITR S2, il quale in questo caso non ha un mapping EID-to-RLOC per 2.0.0.2, e procede incapsulando il pacchetto con l' outer header che consiste nel suo RLOC come source address, copia quindi il destination EID (2.0.0.2) dall' inner header e lo inserisce come destination nell' outer header ; a questo punto instrada il pacchetto (un Data Probe packet) nella LISP-ALT topology, secondo gli schemi implementati dal BGP e arriva infine all' ETR D2.

Quando D2 riceve il pacchetto, lo decapsula e lo spedisce alla destinazione 2.0.0.2, rispondendo con un Map-Reply message per dire ad S2 (11.0.0.1) che l' EID-to-RLOC mapping per 2.0.0.0/8 contiene due elementi: l' ETR D1 (il cui RLOC é 12.0.0.2) e l' ETR D2 (il cui RLOC é 13.0.0.2). Dopo aver ricevuto il Map-Reply message, l' ITR S2 potrá instradare pacchetti in maniera nativa attraverso Internet (senza dover passare per la LISP-ALT Topology).

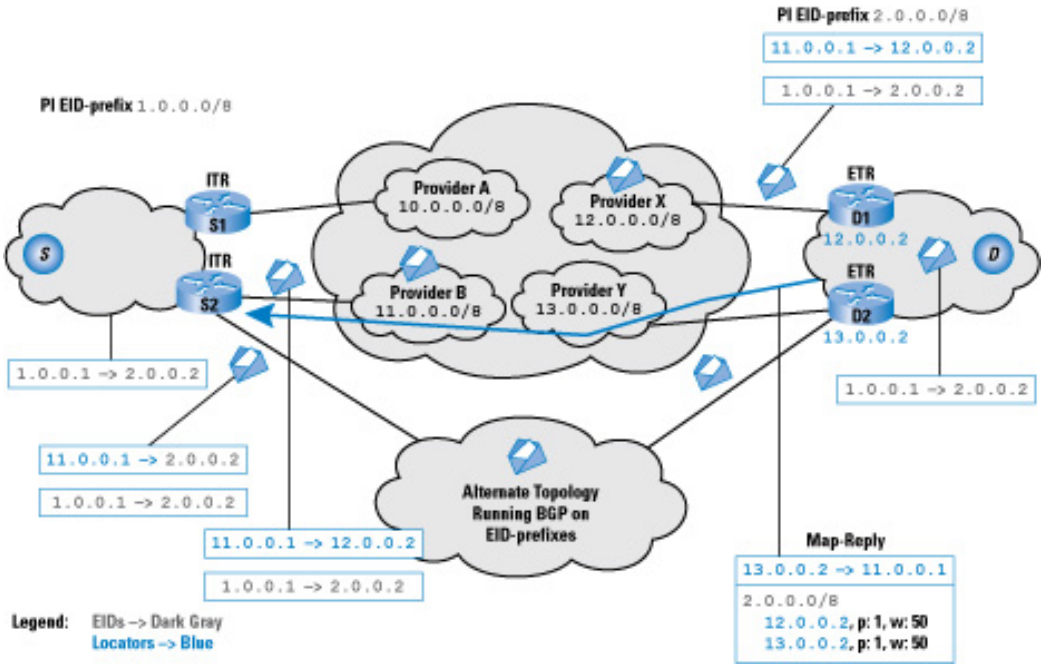

Figura 8.1: A Day in the Life of a LISP Packet

- Note: Il mapping presenta due attributi: prioritá (p) e peso (weight). La prioritá indica all' ITR quali ETRs usare e in quale ordine, e il peso indica all' ITR come suddividere i carichi tra gli ETRs con pari prioritá (w é rappresentato come percentuale di traffico che puó sostenere ogni ETR). In questo caso entrambi gli ETRs hanno la stessa prioritá e peso pari a 50, il ché significa che ognuno di loro é in grado di ricevere il 50 per cento del traffico.

Capitolo 9

Considerazioni

9.1 Nuove Funzionalitá introdotte dal Sistema di Mapping

Pesi e prioritá introducono nuove possibilitá per i multihomed sites, che possono usare queste features per controllare in che modo il traffico in ingresso verso il sito viene distribuito attraverso i suoi links, senza la complessitá e l' overhead riscontrata nel Border Gateway Protocol (BGP).

In particolare, un multihomed site puó configurare il proprio mapping database in modo che i suoi links siano in configurazione active-active (il ché significa che entrambi saranno in uso). Questa situazione, in effetti, é quella raffigurata nell' immagine precedente; in cui il mapping database entry 2.0.0.0/8 ha due ETRs con la stessa prioritá e uguale peso, il ché significa che l' ITR distribuirá equamente i flussi attraverso entrambi gli ETRs. Questa caratteristica risulta particolarmente interessante per Small Office e Home Office (SOHO) sites, i quali aspirano alla ridondanza delle loro internet connections e alla possibilitá di load share attraverso i propri links senza la complessitá e il volume operativo che comporterebbe il BGP.

Un' altra funzionalitá interessante, introdotta dal LISP control Plane, consiste nella possibilitá di contrastare alcuni tipi di DoS Attacks utilizzando i locator-reachability bits per isolarlo.

9.2 Considerazioni sulle performance

LISP e il suo protocollo di mapping evidenziano due principali considerazioni in tema di performance :

- Encapsulation overhead
- EID-to-RLOC lookup latency and packet loss

Per quanto riguarda il primo, si é gia menzionato il fatto che l' aggiunta del LISP header potrebbe causare il superamento dell' MTU in termini di dimensioni del pacchetto incapsulato ; argomento comunque ancora in fase di ricerca.

Per quanto invece concerne la seconda considerazione, é da dire che nonostante il LISP-ALT utilizzi il protocollo BGP per trovare un particolare mapping EID-to-RLOC, e questo comporti una conseguente latenza associata al primo flusso tra siti (si noti infatti che i flussi successivi potranno utilizzare il medesimo mapping situato nell' ITR), questa latenza viene mitigata e il pacchetto iniziale non viene perso poiche LISP é in grado di inviarlo attraverso il Control Plane (si tratta dei Data Probe packets). Messa in conto anche una latenza aggiuntiva dovuta al tempo richiesto dal destination ETR per restituire una Map Reply, nessuna ulteriore latenza sará a carico del mapping sistem. Come visto in precedenza, infatti, LISP-ALT vuole essere una tecnologia push-pull ibrida che punta a diminuire gli state requirements degli ITRs mentre minimizza la latenza dovuta al lookup.

Capitolo 10

Conclusioni

Dopo un' analisi approfondita, e considerando le attuali condizioni della routing scalability, LISP appare come una delle migliori soluzioni per ovviare agli odierni problemi in termini di routing nel contesto di internet. Paragonata alle altre strategie proposte, questa sembra infatti la meglio strutturata; non richiede hardware aggiuntivo per poter funzionare e in piú i costi relativi alla sua implementazione restano al contrario molto contenuti. Proprio perché non sono richieste modifiche strutturali un eventuale introduzione/passaggio a questo nuovo protocollo dovrebbe risultare il piú semplice e indolore possibile. Ci guadagnerebbe inoltre la flessibilitá generale della rete ; dal momento in cui i router si troveranno al di lá di ETRs e ITRs, il numero complessivo di messaggi inviati e ricevuti dovrebbe diminuire, come pure la quantitá di addresses da gestire. Da quanto visionato in precedenza, LISP dovrebbe portare con se una serie di miglioramenti su vari fronti. Da ricordare la riduzione di dimensioni delle routing tables, che insieme alle altre migliorie a carico di ETRs e ITRs sui tempi di processazione, dovrebbero fare di LISP un' architettura un passo avanti a quelle correnti. Questa innovativa Solution, che implementa il Loc/ID split utilizzando un protocollo di map-and-encap, sembra riuscire ad ottenere i vantaggi del livello di indirection raggiunto minimizzando le modifiche richieste e introducendo al contempo funzionalitá inedite, come un BGP-free Multihoming in una configurazione

active-active.

Bibliografia

[1] LISP: Multihoming. http://blog.pattincon.com/

[2] LISP Mobility. http://www.dasblinkenlichten.com/

[3] lisp routing in the cloud. http://lisp.cisco.com/LispUpdate.pdf

[4] IPv6 Transition and Coexistence Using LISP. http://www.cisco.com/

[5] The Locator/ID Separation Protocol. https://datatracker.ietf.org/doc/rfc6830

[6] LISP-Security (LISP-SEC). http://tools.ietf.org/html/draft-ietf-lisp-sec-01

[7] Locator/IDSeparation Protocol (Lisp). http://tools.ietf.org/html/draft-ietf-lisp-23

[8] LISP-Analysi-draft-brim-lisp-analysis-00. https://datatracker.ietf.org/

[9] LISP Functionality. http://www.cisco.com/en/US/products/

[10] LISP: Practice and Experience. https://www.nanog.org/meetings/nanog44/

[11] LISP Threats Analysis draft-ietf-lisp-threats-07. https://datatracker.ietf.org/doc/draft-ietf-lisp-threats

[12] LISP Threats Analysis draft-ietf-lisp-threats-04. http://tools.ietf.org/html/draft-jakab-lisp-deployment-03

[13] LISP: A Level of Indirection for Routing. https://www.nanog.org/meetings/nanog41/presentations/lisp-nanog-abq.pdf

[14] LISP Network Element Deployment Considerations draft-jakab-lisp-deployment. http://tools.ietf.org/html/draft-jakab-lisp-deployment-03

Ringraziamenti

Con queste poche righe voglio cercare di mostrare tutta la gratitudine che provo verso le persone che in questo periodo hanno contribuito al raggiungimento di questo mio traguardo, un traguardo che ha sempre condizionato ogni aspetto della mia vita fin da quando ho memoria.

Dunque, il primo ringraziamento va ad ALLAH, che mi ha sempre aiutata e senza il suo aiuto non c' é l'avrei mai fatta "Alhamdolilah".

Vorrei ringraziare i miei genitori Hassan e Jamila per il loro sostegno fino dal primo giorno in cui sono arrivata in Italia, per avermi dato l' opportunitá di poter conseguire la laurea nell' universitá di Bologna, per essermi stati sempre vicini anche se sono lontani, per avermi incoraggiata e sostenuta nelle mie scelte. Grazie papá perché hai sempre avuto fiducia in me e mi hai sostenuta sempre e comunque ,grazie mamma per le tue preghiere prima di ogni esame, per aver creduto sempre in me, per avermi sostenuta sia nei momenti di difficoltá sia in quelli felici e spensierati. Vorrei anche dirvi che senza di voi non sarei mai diventata quello che sono e non avrei potuto coronare i miei molteplici sogni e spero di non avervi mai delusa e che voi possiate essere orgogliosi di me. Grazie a mia sorella Yousra che c' é stata sempre vicino a me nella mia avventura, dal primo giorno in Italia, fino a questo giorno e spero che l'imminente inizio della sua avventura a Milano possa essere altrettanto felice come quella che ho vissuto io Bologna, grazie sorellina per avermi sopportata. Vorrei anche ringraziare i miei fratellini Mohamed e Zineb per il loro sostegno in lontananza per esservi sempre interessati all' esito dei miei esami, per aver percorso questo cammino anche voi con me.

Vorrei dedicare questa tesi anche a mia nonna, una nonna non come le altre coraggiosa e che combatte fino ad arrivare al suo obbiettivo, ci hai sempre insegnato a resistere e combattere per il suo proprio sogno, anche se adesso non ci sei piú vorrei ringraziarti, se oggi sono qui a scrivere questa tesi e anche merito tuo mi hai sempre motivata e incoraggiata per arrivare fino alla fine, nonna non ti scorderemo mai.

Ringrazio Giuseppe, che dopo un inizio tormentato é riuscito a rendere docile il mio caratteraccio, il quale con estrema pazienza ha sopportato i miei sbalzi di umore e le mie paranoie quando, sotto stress per un esame, non avevo altra valvola di sfogo che lui, mi ha sempre incoraggiata dicendomi che potevo farcela. Lo ringrazio perché ha sempre trovato un modo di farmi sorridere. Oggi se cé l' ho fatta é anche merito tuo.

Ringrazio innanzitutto il mio prof e relatore di questa tesi, prof Vittori Ghini per la disponibilitá e la cortesia avute nei miei confronti, e per avermi consigliato un tema cosí interessante e ambizioso, nonché per la schiettezza, le opportunitá datomi e l' entusiasmo dimostratomi. Lo ringrazio per avermi dato la possibilitá di confrontarmi con nuovi e stimolanti argomenti come questo.

Ringrazio il mio miglior amico di sempre Abdes, per avermi accompagnata in tutto questo viaggio con il sorriso, sia nei momenti tristi sia quelli belli, non scorderó mai i giorni passati con te nelle aule studio e i lab.

Ringrazio la mia miglio amica Roby, per tutto quello che ha fatto per me, e per la sua pazienza infinitá ad ascoltarmi tutti i venerdi sera.

Mi sento un puó emozionata e allo stesso tempo terrorizzata di dimenticare qualcuno di realmente importante. Io ci provo, e spero di non dimenticarmi di nessuno. Fatti e persone, che hanno reso la mia avventura cosí bella fino ad oggi, meriterebbero peró un libro, ringrazio i miei cari e splendidi amici e colleghi dell' universitá per aver passato con loro dei bei momenti, in particolare ringrazio Ivan per i suoi consigli e i suoi appunti, il mio amico Youssef, Luca Giuliano, Riccardo di Tosto e molti altri, dalle cui sorprendenti manifestazioni di affetto ho tratto la forza per superare i momenti piú

difficili, é stato molto bello conoscervi e condividere con voi ogni momento dell'univertá.

Grazie a tutti voi per essermi stati vicini.

Hassna.